Data Retention Legislation – Privacy Impact Assessment

1 July 2014

1. Executive summary

This document is the Privacy Impact Assessment (PIA) for the implementation of proposed data retention legislation to recreate the provisions of the Data Retention (EC Directive) Regulations 2009. The purpose of this PIA is to: consider the privacy impact of the proposed legislation; assess whether the capabilities implemented through this proposed legislation will be compliant with the Data Protection Principles (DPP) and the Data Protection Act 1998 (DPA).

This Privacy Impact Assessment (PIA) follows the approach and guidelines recommended by the Information Commissioner's Office (ICO). It considers the impact on privacy of the proposed data retention legislation: communications data is regarded as personal data as defined by the Data Protection Act 1998.

The new legislation will replicate the mandatory communications data retention regime of the Data Retention (EC Directive) Regulations 2009. As the status quo is simply being restored, there will be no impact upon privacy beyond that which existed under previous mandatory regime.

Nevertheless, this PIA identifies the risks to privacy arising from the capabilities that will continue to be available under the new legislation, and sets out the safeguards, existing and new, intended to address these risks (section 4). The PIA concludes with a Privacy Impact Statement (see section 5).

2. The case for legislation

2.1 Rationale

Communications data (CD) is the context, not the content of a communication: who was communicating; when; from where; and with whom. It includes the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the 'what' – i.e. the content of any communication – the text of an email or a conversation on a telephone. Communications data is defined in the Regulation of Investigatory Powers Act 2000 and is legally distinct from a communication's content.

Communications data is absolutely fundamental to ensure law enforcement have the powers they need to investigate crime, protect the public and ensure national security. It is used by the police and intelligence agencies in the investigation of many types of crime, including terrorism. It enables the police to build a picture of the activities, contacts and whereabouts of a person who is under investigation.

It has also played a significant role in the investigation of a very large number of other serious and widely reported crimes, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman, the 2007 Glasgow Airport terror attack, and the murder of Rhys Jones. Where an investigation starts with an internet communication, such as in online child sexual exploitation cases or identifying the location of people at risk of imminent harm, communications data will often be the only investigative lead. If this data is not retained, these cases will go unsolved.

Communications data is also regularly used in court, and was used in 95% of all serious and organised crime investigations handled by the Crown Prosecution Service between July 2012 and February 2013.

The retention of communications data in the UK has been recognised as a valuable and important measure for a number of years. Access to communications data by law enforcement and the security and intelligence agencies (and other relevant public authorities) is primarily regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA places strict rules on when, and by whom, data can be obtained and provides authorities with a framework for acquiring communications data which is consistent and compatible with the European Convention on Human Rights (ECHR). The processing of personal information, including communications data, and the storage of personal data by industry is also subject to the Data Protection Act 1998 (DPA).

The UK Government first introduced legislation on communications data retention in 2001. The Anti-Terrorism, Crime and Security Act 2001 (ATCSA) included at Part 11 provisions for a voluntary regime for the retention of communications data by communications companies for longer than they would otherwise have done.

The EU Data Retention Directive (Directive 2002/58/EC) passed into EU law in March 2006. This required European Member States to implement legislation into their own national law requiring communications companies to retain specific communications data sets for retention periods between 6 and 24 months.

The EU directive was initially transposed into UK law for telephony only by the Data Retention (EC Directive) Regulations 2007. These were updated to include internet communications by the Data Retention (EC Directive) Regulations 2009 (DRR). These Regulations required UK communication providers to retain certain specified types of telephony and internet related communications data which was generated or processed in connection with their business for 12 months.

On 8 April 2014, the European Court of Justice issued a judgment determining that the Data Retention Directive was not compatible with EU Charter Rights and was therefore invalid.

The ECJ judgment drew attention to:

- The broad nature of the Data Retention Directive and the blanket nature of data retention, as interpreted by the Court.
- The lack of safeguards in the Directive around access to data retained under it.
- The lack of objective grounds and decision making that Member States must go through to ensure that any data retention obligation is limited to what is necessary.
- The obligations placed on Member States by the Directive to ensure appropriate data security exists for any retained data were insufficient.

The UK has one of the best communications data oversight and authorisation systems in the world. We believe that our retention and access regime already meets most of the ECJ's criticisms. Under RIPA, access to communications data is subject to a set of stringent safeguards. The Joint Committee on the Draft Communications Data Bill looked at this regime in detail and concluded that "the current internal authorisation procedure is the right model".

Despite the judgment, the UK Data Retention (EC Directive) Regulations 2009 are considered to remain in force. Communications service providers in receipt of a notice under the Regulations were informed that they should continue to observe their obligations as outlined in any notice.

We consider this legislation to be the most effective way of ensuring that our communications data retention regime, when combined with the access regime provided for by Part I Chapter II of RIPA, effectively address the opinions of the ECJ judgment on the Data Retention Directive.

Intervention is necessary to ensure the continued availability of this data. The retention of communications data is absolutely fundamental to ensure law enforcement have the powers they need to investigate crime, protect the public and ensure national security. We must ensure we maintain an effective data retention regime in the UK so that communications data continues to be available to law enforcement for longer than the three months that it is normally retained by communications service providers for business purposes. If communications data was not retained for more than three months, law enforcement's capability to prevent and detect crime and protect the public would be severely degraded; many investigations would be delayed and some would cease entirely.

2.2 Strategy

This legislation is a key part of the future strategy to maintain the availability of communications data for the protection of the public and public safety.

The strategy is informed by close engagement with: the users of communications data, notably the police, law enforcement and intelligence agencies; and the communications service providers (CSPs) whose services generate data and whose technology is essential in making data available.

2.3 Overview of the proposed legislation

The objective of this legislation is to restore the status quo, replicating the retention requirements of the Data Retention Regulations, whilst also addressing the opinions of the European Court's Judgment.

The legislation will not address the ongoing erosion of capabilities arising from the migration of communications from fixed line and mobile telephones to the internet.

3. Overview of current and planned safeguards

The UK currently has in place one of the best communications data oversight and authorisation systems in the world.

In meeting the European Court Judgment's opinions where possible, the new legislation (in the form of primary legislation and supporting regulations) will go further in safeguarding human rights. These additional safeguards will include:

- Specifying that Ministers must consider the necessity and proportionality before issuing a notice to a communications service provider.
- Specifying further requirements around what information Ministers must consider before issuing a data retention notice.
- Amending the set period for which data is retained, from 12 months to a maximum of 12 months (allowing for shorter periods if there is lesser need).
- Limiting access to retained communications data to requests under RIPA and court orders.
- Ensuring that specific data security requirements must be specified in a notice to each CSP when it is issued, rather than in commercial arrangements as at present.
- Clarifying in the legislation the duties of the Information Commissioner, so that he can oversee all of the relevant aspects of the retention of data (including data integrity and destruction).

We consider that these new safeguards, in addition to those already existing, provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy.

4. Privacy Risks

The new mandatory data retention regime will not have any greater impact on privacy than the old mandatory regime, and in some areas it will introduce additional safeguards. However, this section considers the impact on privacy of the new regime, and sets out the relevant existing and proposed safeguards.

4.1 The risk that the scope of data retention by CSPs will unnecessarily and disproportionately intrude on privacy

It is in the business interests of CSPs to maintain the integrity of the data they use. With respect to personal data such as communications data, the principles in the Data Protection Act 1998 require them to do so. Testing regimes ensure that only valid and accurate communications data is retained. In addition, existing and proposed legislation provide substantive safeguards.

Under the new legislation, Ministers must consider the necessity and proportionality of issuing a notice on a communications service provider before anything else.

Continuing Safeguards

The Data Protection Act 1998 provides safeguards with respect to data retention. The Act gives the Information Commissioner's Office (ICO) powers which help protect personal data including communications data. The ICO can:

- conduct assessments to check organisations are complying with the DPA;
- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- serve enforcement notices and 'stop now' orders where there has been a breach of the DPA, requiring organisation to take specified steps to ensure they comply with the law;
- prosecute those who commit criminal offences under the act;
- report to Parliament on data protection issues of concern; and
- serve notices requiring organisation to pay up to £500,000 for serious breaches of the DPA.

Under the DPA, it is a criminal offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal information without the consent of the data

controller. An employee of a public authority or a CSP would commit such an offence if they illegally obtained communications data. It is also an offence to sell or offer to sell illegally obtained personal information.

Furthermore, the purposes for which communications data may be acquired in order to protect the public are set out in RIPA, and are entirely consistent with Article 8(2) of the European Convention on Human Rights. Parliament designates which public authorities can obtain communications data under RIPA, and for which purposes. RIPA requires requests for data to be approved by senior officials or officers in the applying agency. Approval may only be given if an applicant is able to demonstrate that data is necessary in an investigation for a permitted purpose and proportionate to the objective of the investigation: an application must assess the benefits of the data which has been requested against intrusion into privacy. Since November 2012, local authorities also need to get the approval of a magistrate under new provisions in the Protection of Freedoms Act 2012.

New safeguards

The impact on privacy will be further reduced as a result of a number of new safeguards (in primary legislation and/or subsequent regulations):

- The legislation will specify that Ministers must consider the necessity and proportionality of issuing a notice on a communications service provider. This judgement will be based upon the ECHR-compliant statutory purposes that already exist in RIPA in relation to data acquisition.
- It will also specify further requirements around what information Ministers must consider before issuing a data retention notice. It will also contain a requirement to keep these notices under review.
- The set period for which data is retained will be amended, from 12 months to a maximum of 12 months. This will allow data to be retained for shorter periods if there is lesser need to do so.
- Access to retained data will be restricted on the face of the legislation to RIPA and court orders.
- Clarifying in the legislation the duties of the Information Commissioner, so that he can oversee all of the security and integrity of aspects of the retention of data.

4.2 The risk of unauthorised use or mishandling of communications data retained by CSPs

There is a risk that CSPs could use without authorisation or otherwise mishandle the communications data they retain. It is possible, for example, that data on customers

might be lost or misused or that data held under the new legislation might be exploited for business purposes.

Continuing Safeguards

Under the DRR, a set of physical, procedural and technical safeguards were put in place to prevent unauthorised access to systems in CSPs. Access controls provide users with rights and/or privileges to access and perform functions. Controls should enable authorised users to access the minimum necessary information to perform their roles. Access controls include, but are not be limited to, unique user identification, automatic logoff and encryption/decryption of credentials and requests. Such controls will also be required under these provisions.

Someone who knowingly accesses a computer system that they are not authorised to access in order to obtain or disclose communications data may commit an offence under the Computer Misuse Act 1990. Offences under this Act can carry a term of imprisonment up to two years.

Under the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR), the Information Commissioner's Office has the power to audit the measures taken by CSPs to safeguard personal data. The powers under the PECR only allow the ICO to audit security measures and do not cover the power to audit retention of information (although they do allow the ICO to audit measures taken to ensure personal data is not being unlawfully processed).

New safeguards

The risk that CSPs could use without authorisation or otherwise mishandle the communications data they retain will be mitigated by a number of the new safeguards (in primary legislation and/or subsequent regulations):

- The legislation specifies that specific data security requirements must be set out in a notice to each CSP when it is issued. This will go further than the current system, in which these requirements are set out by way of a commercial arrangement.

- The Information Commissioner's duties will be clarified in the new regulations to ensure that he can audit the compliance by CSPs of the security and integrity requirements. By auditing, he will ensure that standards are maintained.

4.3 The risk that communications data held by CSPs is not appropriately secured or protected from unauthorised access

There is a risk that through a breach of security, communications data held by CSPs could be obtained by an unauthorised third party.

Continuing Safeguards

Data security requirements originally set out in the DRR are replicated in these provisions. The DRR specified that retained data must be subject to technical and physical controls to prevent access by unauthorised personnel (i.e. access is limited to the team that deal with disclosures and can't be accessed by others in the organisation). To ensure the secure retention of communications data, the Government sets out 37 specific security measures further to requirements in the directive. These criteria are based on the government's Security Policy Framework and Information Assurance Standard 1&2. Both of these documents are publically available and align HMG with the international security standard ISO:IEC 27001:2013. The Government reinforces the application of the security measures by a process of compliance visits and provision of security advice.

RIPA also sets a set of stringent safeguards relating to access to retained data. This model centres on a trained and accredited Single Point of Contact in each law enforcement agency, who acts as guardian and gatekeeper, ensuring that data is only acquired when necessary and proportionate to do so for a specific investigation. Requests for data are then assessed and, if appropriate, approved by a senior officer, of a rank designated by Parliament. The Joint Committee on the Draft Communications Data Bill looked at this regime in detail and concluded that "it is our view that the current internal authorisation procedure is the right model."

Only public authorities designated by Parliament can obtain communications data under RIPA for those purposes set out by Parliament. The list of authorities and purposes are set out in legislation. Law enforcement and intelligence agencies account for 99% of requests for communications data. Some other public bodies, including some Government Departments, regulators and local authorities, have been granted access to some communications data under RIPA in order to discharge their investigatory or public protection responsibilities. Since November 2012, local authorities need to get the approval of a magistrate under new provisions in the Protection of Freedoms Act 2012.

New safeguards

The risk that data held by CSPs could be obtained by an unauthorised third party will be mitigated further. Access by public authorities to communications data retained under the new legislation will on the face of the legislation be solely on the basis of RIPA requests or court orders.

The Information Commissioner, who already oversees the security of retained data, will have his duties clarified in the new legislation.

4.4 The risk that communications data is not destroyed by CSPs

There is a risk that, as equipment is decommissioned and retention periods expire, data is not properly destroyed, which will lead to a breach of the DPA.

Continuing Safeguards

Provisions for the deletion of data in the DRR will be replicated. Data must be deleted at the end of the retention period, subject to any extension for the purpose of legal proceedings. This is overseen by the Information Commissioner.

New safeguards

As previously stated, the Information Commissioner will have his duties clarified in the new regulations.

5. Privacy Impact Statement

This Privacy Impact Assessment has been carried out to assess the risks to privacy posed by the work carried out on the basis of the proposed legislation. It is assessed that implementation of the proposed legislation is capable of being fully compliant with the Data Protection Principles and the Data Protection Act.

5.1 Data Controllers and Data Processors

The data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is or will be processed. The data controller for personal data depends on where it is being stored/processed during the communications data retention/acquisition/disclosure process.

Under the new regime, as under the old one, CSPs will be the data controllers until the point where the retained data is disclosed to the public authority, when the public authority will become the data controller of the obtained communications data.

5.2 Subject Access Requests

The Data Protection Act gives the subjects of data the right to request access by making a Subject Access Request (SAR). An exemption to this exists for personal data that is being processed on the grounds of national security or for the "prevention or detection of crime" but only to the extent that complying with a particular request would prejudice the prevention and detection of crime. SARs are determined on a case by case basis and not subject to blanket exemptions.

A SAR made of a public authority would be exempt from disclosure if compliance would prejudice the prevention or detection of crime. This might for example occur if by disclosing that an authority held communications data on an individual that would

indicate that an investigation is underway. However, a SAR could be made of the data retention store itself.